Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

Policy Area: Security	**Policy #:** ITD-SEC-3.00
Title: Enterprise Electronic Messaging Communications Security Policy	**Effective Date:** February 6, 2003

Issue Statement
Electronic communication includes any communication that is transmitted, acknowledged, stored, downloaded, displayed, or printed by an electronic communication system or service. Given the ubiquitous nature of electronic communication, critical to Commonwealth agencies' and organizations' ability to provide efficient constituent support, this policy focuses on the specific category of electronic messaging (i.e., email, instant messaging, etc.) communication and related threats that, if left unmitigated, may lead to a loss of data and/or system integrity, confidentiality, or availability.

The Commonwealth's Position
Commonwealth agencies and organizations must continue to strive for electronic messaging communications reliability, availability, integrity, and performance by supporting enterprise and local agency efforts including, but not limited to, the following:

Enterprise Filtering
ITD currently filters Internet - MAGNet inbound and outbound email as follows:

1. Known Viruses: subject line, message body, and attachment(s). Emails containing files with extensions, which are affiliated with a virus, are discarded. Users must be aware that emails containing executables may be discarded.
2. Content Spam: Including subject line and/or specific spam content, requested by an agency or otherwise identified as spam.
3. RFC 2822 (see: http://www.faqs.org/rfcs/rfc2822.html): a standard specifying acceptable syntax for text messages sent between computer users, within the framework of "electronic mail" messages.
4. Message Segmentation: All multi-part MIME messages will be blocked at the gateway. Message segmentation allows a large message to be divided up into smaller messages for transmission. Unfortunately these smaller messages may hide viruses and other malicious software. Therefore, message segmentation is banned.

Please Note: MAGNet-inbound Internet sourced email - including replies back to a MAGNet mail account message source - are scanned by filtering software.

Commonwealth Agency & Organization Filtering
Non-MassMail Agencies may continue to deploy local content filtering technology that screens agency-specific transmission of email, subject to restrictive attributes defined by each agency. Agencies that have documented that they have adopted and distributed to all new and current employees an acceptable use policy that states that employees have no expectation of privacy in their workplace email can content filter outgoing employee email with minimal risk of violating employees' privacy rights. Even in agencies that have such documentation, content filtering incoming email poses the risk of violating outside parties' rights under the Commonwealth's Privacy Law, Mass. Gen. L. ch. 214, and Wiretap Statute, Mass. Gen. L. ch. 272, sec. 99. Agency counsel should consult ITD's General Counsel prior to advising their clients that they may content filter incoming electronic mail.

Private Email Accounts
Since the use of private email (i.e., a commercial email system or service, separate and apart from an agency's primary email system) has been a primary source of unauthorized intrusion (e.g., virus instantiation), it is not allowed within MAGNet. Agencies found to be the source of a

virus, distributed denial of services attack, or otherwise unauthorized intrusion, due to the use of private email, may be disconnected from MAGNet until such use has been discontinued.

Instant Messaging
The use of "Public" Instant messaging (IM), including but not limited to, Internet Relay Chat (IRC), I Seek You (ICQ), and AOL Instant Messenger (AIM), has been exploited as an unauthorized intrusion channel (e.g., denial of service attack). Therefore use of IM is not allowed within MAGNet.

Exception Requests
If an agency or organization determines that the use of private email and/or Instant Messaging is critical to its mission, the agency head or their designee must request an exception to this policy. Such a request must document reasons the exception is required, under what circumstances, duration, and access controls that will ensure that the agency has taken sufficient steps to mitigate or isolate the associated threat, (e.g., how email account users are prevented from simultaneous access to the agency's default email and private email accounts). Documented requests for exceptions must be submitted to ITD and the Enterprise Security Board for review and approval prior to agency implementation.

Commonwealth Agency/Organization and User Responsibilities
Agency Head Responsibility
Agency Heads and/or their designees are responsible for ensuring that employees, contractors, and/or business partners that may be affected, are aware of this policy.

User Responsibility
Commonwealth agency and organization users must not introduce electronic messages, which may damage the local or enterprise (MAGNet) environment. Items, which could be considered a detriment, include, but are not limited to viruses, distributed denial of service attacks, Trojans, Worms, and/or personal electronic communications contributing to network congestion.

If the user does not know the sender of an email, the recipient should determine if the email should be deleted without opening it. The recipient may telephone the sender to ask if the email is legitimate. The recipient may also consult CommonHelp.

The user should have their email configured so that an email is not automatically opened when a previous email is closed, deleted or moved.

Additional Legal Issues
All electronic messages created or received by state employees using the Commonwealth's information technology resources are public record under the Commonwealth's Public Records Law, Mass. Gen. L. ch. 66, sec. 10, and most are therefore subject to public scrutiny. All such electronic messages are also records subject to the Commonwealth's Records Conservation Law, Mass. Gen. L. ch. 30, sec. 42, and must be disposed of, or retained according to the agency's disposition schedule and the Commonwealth's Records in Common disposition schedule. Most such messages are also potentially discoverable communications for purposes of litigation. Thus Agency heads and organization authorities must ensure that all electronic communications, are retained, disposed of, and disclosed, in compliance with the Public Records Law, the Records Conservation Law and the relevant discovery rules.

Compliance
Agencies within the Executive Department must comply with this Enterprise Electronic Messaging Communications Security Policy. All Commonwealth agencies and organizations must comply with this policy as a prerequisite for access to and/or participation within MAGNet, and/or to use information resources managed by ITD. Vendors, who seek to work with any agency or organization within the Commonwealth of Massachusetts, must comply with this and all the Commonwealth's Enterprise Security Policies, Standards and Procedures as published by ITD.

Supplementary Information

- Enterprise Security Policies
  http://www.itd.state.ma.us/spg/publications/standards/index.htm
- Commonwealth Public Access Architecture
  http://www.state.ma.us/itd/spg/publications/standards/standards.htm
- ITD Messaging Architecture and Enterprise Standards
  http://www.state.ma.us/itd/spg/publications/standards/archstan.htm - messaging

Points of Contact

- CommonHelp (866)888-2808 commhelp@state.ma.us ITD-DL - COMMON HELP
- Chief Information Security Officer, ITD
- Enterprise Security Board
- General Counsel, ITD